

SZEMFÉNYVESZTŐK A HÁLÓZATON

MIÉRT TUDUNK SIKERREL JÁRNI?



Veres-Szentkirályi András 2019-07-19



Veres-Szentkirályi András

- ▶ OSCP, GWAPT, SISE
- ▶ Silent Signal alapító
- ▶ pentester, toolmaker

Menetrend

- 1 Bevezetés
- Hozzáállás
- Egy a jelszó: tartós béke
- Humán faktor
- Kedves naplóm!

Egy fontos gondolat előszó helyett



“Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can’t break.”

– Bruce Schneier (1998. október 15.)

<https://www.schneier.com/crypto-gram-9810.html#cipherdesign>

Grand Brighton Hotel, 1984



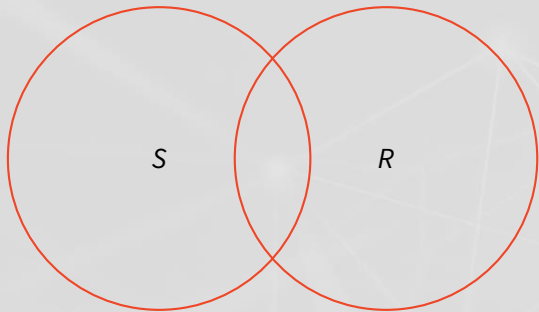
“Today we were unlucky, but remember **we only have to be lucky once. You will have to be lucky always.**”

– Provisional IRA (1984. október 13.)

Taylor, Peter (2001). Brits: The War Against the IRA.
Bloomsbury Publishing. p. 265. ISBN 0-7475-5806-X.

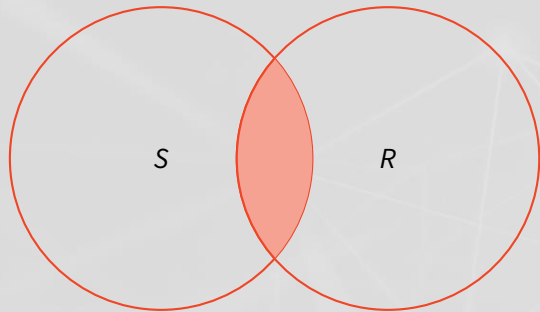
https://en.wikipedia.org/wiki/Brighton_hotel_bombing

Offenzív vs. defenzív megközelítés



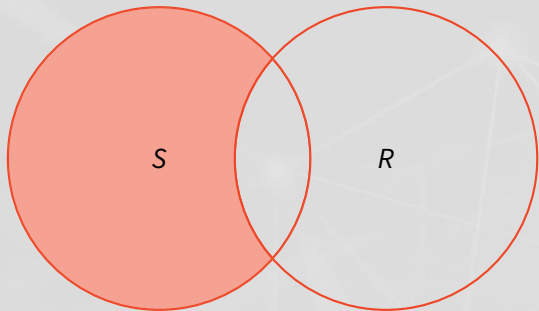
- ▶ *S* specifikáció
- ▶ *R* rendszer

Offenzív vs. defenzív megközelítés



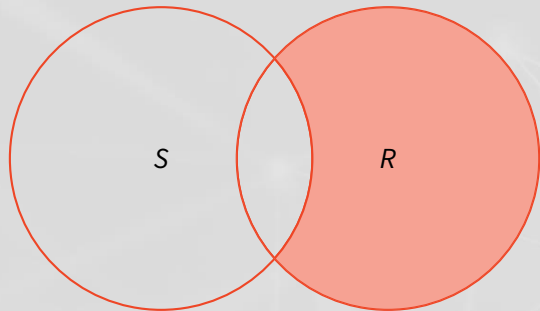
- ▶ S specifikáció
- ▶ R rendszer
- ▶ $S \cap R$ specifikációnak megfelelően működő rendszer (ideálisan $S = R$)

Offenzív vs. defenzív megközelítés



- ▶ S specifikáció
- ▶ R rendszer
- ▶ $S \cap R$ specifikációnak megfelelően működő rendszer (ideálisan $S = R$)
- ▶ $S - R$ specifikációban szereplő, de rendszer által **nem** nyújtott szolgáltatás
 - ▶ bug, funkcionális hiba

Offenzív vs. defenzív megközelítés



- ▶ S specifikáció
- ▶ R rendszer
- ▶ $S \cap R$ specifikációnak megfelelően működő rendszer (ideálisan $S = R$)
- ▶ $S - R$ specifikációban szereplő, de rendszer által **nem** nyújtott szolgáltatás
 - ▶ bug, funkcionális hiba
- ▶ $R - S$ specifikációban **nem** szereplő, de rendszer által nyújtott szolgáltatás
 - ▶ feature, potenciális biztonsági hiba

Menetrend

- Bevezetés
- **Hozzáállás**
- Egy a jelszó: tartós béke
- Humán faktor
- Kedves naplóm!

Mi rossz történhet? (©HBO)

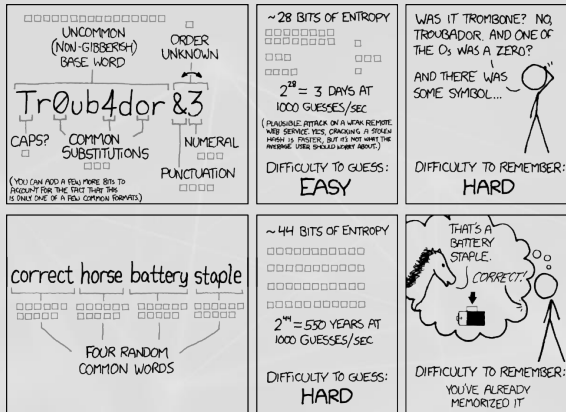


- ▶ Védő: véges erőforrások
- ▶ Támadó: véges erőforrások
- ▶ $R - S$ halmaz
 - ▶ portok / tűzfalszabályok
 - ▶ ACL / sudoers bejegyzések
 - ▶ SUID binárisok
- ▶ Proaktív megközelítés: RDP NLA
 - ▶ MS12-020
 - ▶ CVE-2019-0708

Menetrend

- Bevezetés
- Hozzáállás
- 3 ● Egy a jelszó: tartós béke
- Humán faktor
- Kedves naplóm!

Kommentár nélkül (<https://xkcd.com/936/>)



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Jelszókomplexitás (©HBO)



NIST ajánlások 2017 júniusából



- ▶ ajánlott olvasmány: <https://pages.nist.gov/800-63-3/sp800-63-3.html>
- ▶ nem javasolt a periodikus jelszólejjárát
- ▶ nem javasolt a komplexitási borzalom
- ▶ nem javasolt korlátozni a komplexitást és a jelszó hosszát
- ▶ javasolt gyakori/kompromittált jelszavak listájával összevetni

NIST ajánlások 2017 júniusából

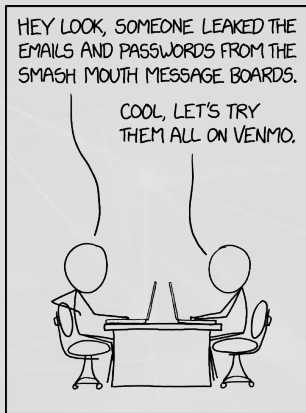


- ▶ ajánlott olvasmány: <https://pages.nist.gov/800-63-3/sp800-63-3.html>
- ▶ nem javasolt a periodikus jelszólejtár
 - ▶ Sysadmin: változtass havonta jelszót!
 - ▶ Felhasználó: Kiskutya1907
- ▶ nem javasolt a komplexitási borzalom
 - ▶ Sysadmin: kisbetűnagybetűszámspeciáliskarakter (egy levegővel)
 - ▶ Felhasználó: Be1@1988
- ▶ nem javasolt korlátozni a komplexitást és a jelszó hosszát
 - ▶ vajon mit mond el egy háttérrendszerről, hogy nem képes tetszőleges hosszúságú és összetételű jelszót kezelni?
 - ▶ nyílt szövegű jelszó tárolása? injection?
- ▶ javasolt gyakori/kompromittált jelszavak listájával összevetni

Hétfőn érkezett [\(https://xkcd.com/2176/\)](https://xkcd.com/2176/)



HOW PEOPLE THINK
HACKING WORKS

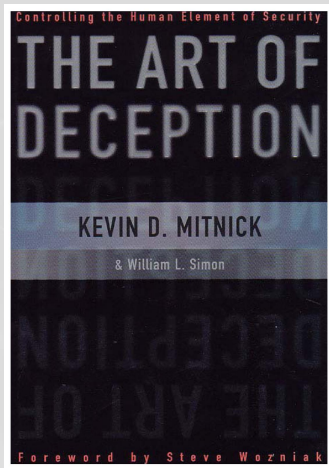


HOW IT ACTUALLY WORKS

Menetrend

- Bevezetés
- Hozzáállás
- Egy a jelszó: tartós béke
- 4 Humán faktor
- Kedves naplóm!

Biblia?



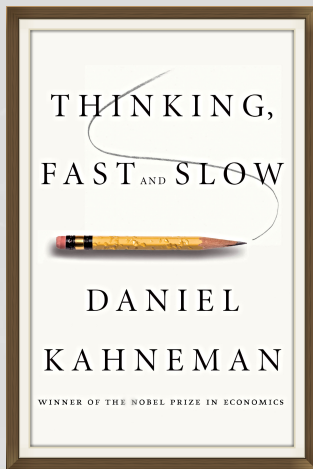
Tetszőleges broken OPSEC anyagból



- ▶ figyelj az URL-re, különben phishing támadásnál megadod jelszavad
 - ▶ <https://silentsignal.hu/>
- ▶ ne nyiss meg megbízhatatlan forrásból származó levelet/csatolmányt
 - ▶ #define megbízhatatlan
 - ▶ és dolgozni ki fog?

Ne erőltessük

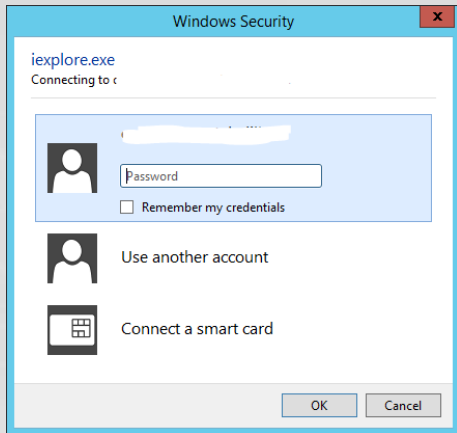
?



Műszaki megoldások: prevenció



- ▶ levelek egyértelmű automatizált besorolása
 - ▶ SPF
 - ▶ DKIM
 - ▶ DMARC
- ▶ Mire szoktatjuk a felhasználókat?
 - ▶ „szokott ilyen autentikációs ablak csak úgy felugrani”
 - ▶ „SSL tanúsítvány hiba? már rutinból kattintok is...”
- ▶ <https://blog.silentsignal.eu/2019/04/04/our-take-on-social-engineering/>



Műszaki megoldások: modern 2FA



Műszaki megoldások: risk mgmt



- ▶ cukorka biztonság
- ▶ defense in depth
- ▶ sikeres ransomware kampányok

“For the same reason our reactors **do not have containment buildings around them**, like those in the West. [...] **It’s cheaper.**”

©HBO



Menetrend

- Bevezetés
- Hozzáállás
- Egy a jelszó: tartós béke
- Humán faktor
- 5 Kedves naplóm!

- ▶ majd ha más forrásból kiderül valami, jól belenézünk?
- ▶ mi kerül bele?
- ▶ mit vált ki egy-egy bejegyzés?
- ▶ valós példa:
 - ▶ inaktív felhasználót aktiválnak (napi rendszerességű): riasztás
 - ▶ domain admin jön létre (nagyon ritka és veszélyes): csend
- ▶ SNR?

- ▶ Ne csak „magunk ellen” védjük a rendszert!
- ▶ Gondoljunk arra, hogy mindig lesz olyan, aki nem tartja be a játékszabályokat!
 - ▶ sőt, tőlük kellene igazán védenie a rendszernek
- ▶ Nyessük le a plusz „feature”-öket!
- ▶ A biztonság is legyen része a formalizált-automatizált minőségbiztosítási rendszernek!
 - ▶ a sebezhető rendszer színtelen és szagtalan

KÖSZÖNÖM!

VERES-SZENTKIRÁLYI ANDRÁS

vsza@silentsignal.hu



facebook.com/silentsignal.hu



@SilentSignalHU



@dn3t

